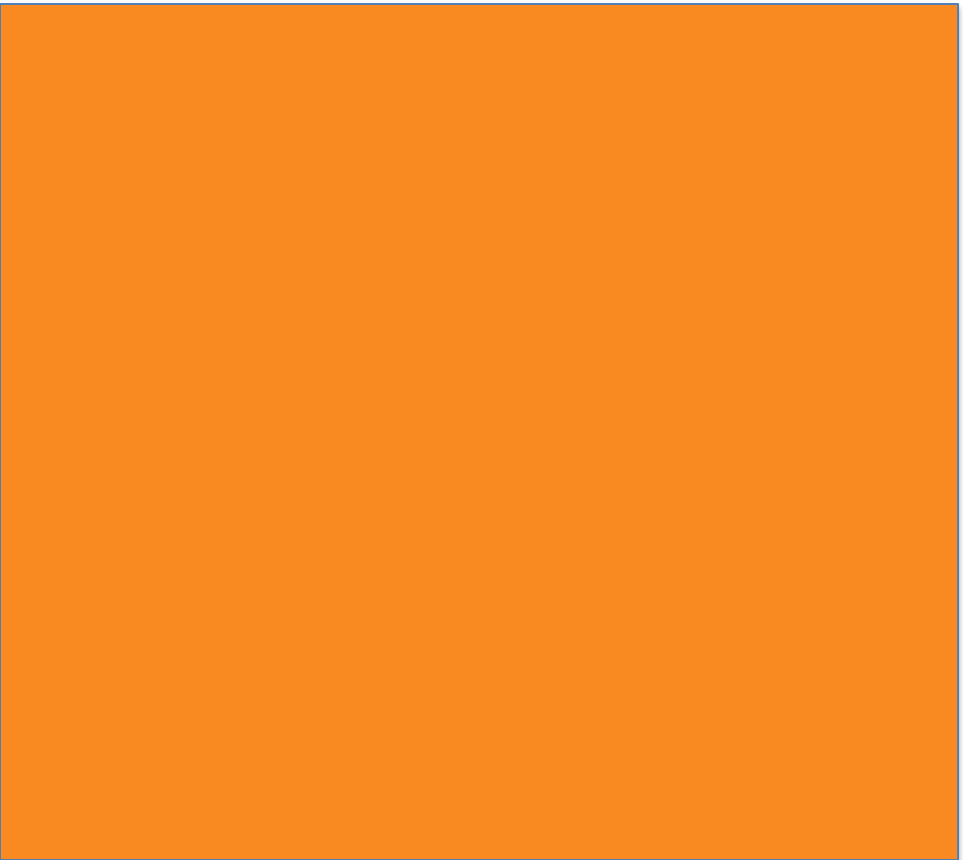


Un mundo en ciberguerra. ¿Cómo gestionar una violación de ciberseguridad? ¿Qué hacer ante un ataque?

Antonio Ramos

20 mayo2015

CSX™
CYBERSECURITY NEXUS

Responding to Targeted Cyberattacks

ISACA
www.isaca.org/cyber

ERNST & YOUNG

Advanced Persistent Threats

How to Manage the Risk to Your Business

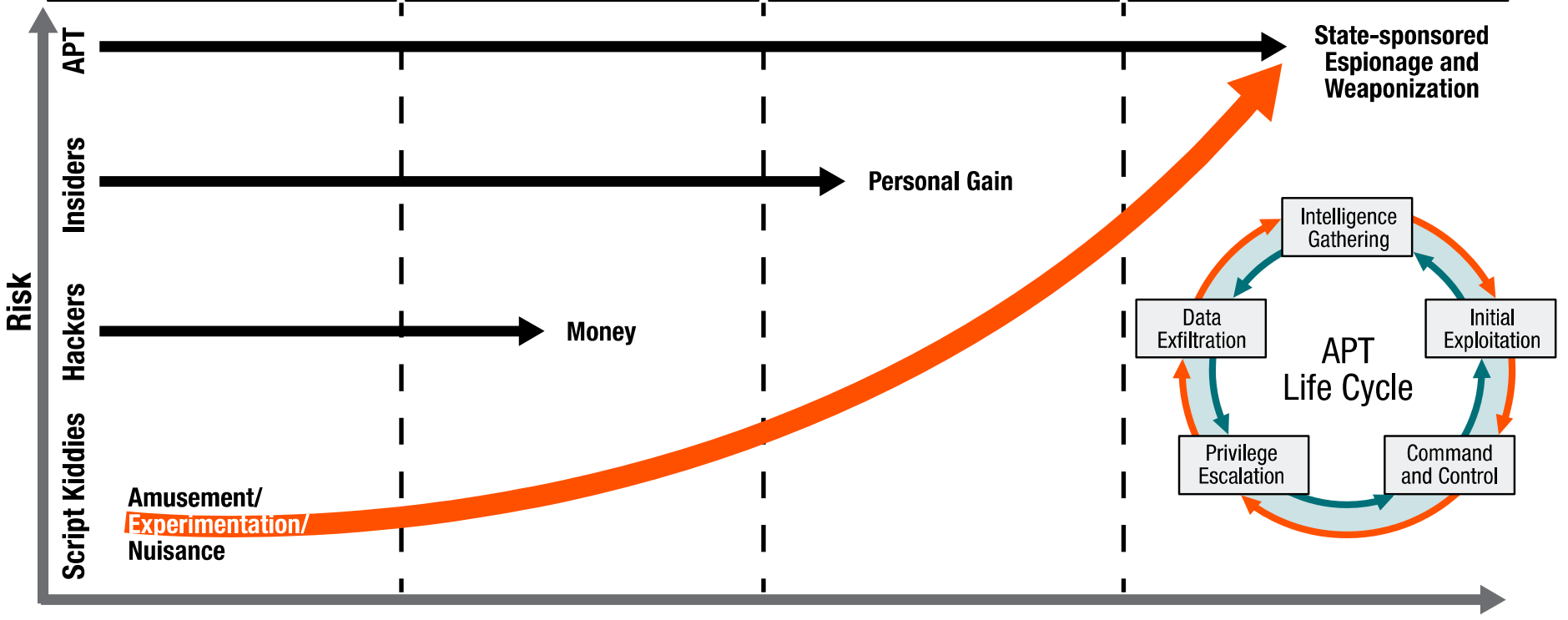
Evolución del escenario de amenaza

Unsophisticated Attackers (Script Kiddies)
You are attacked because you are on the Internet and have a vulnerability.

Sophisticated Attackers (Hackers)
You are attacked because you are on the Internet and have information of value.

Corporate Espionage (insiders)
Your current or former employee seeks financial gain from seling your IP.

State-sponsored Attacks Advanced Persistent Threat (APT)
You are targeted because of who you are, what you do, or the value of your IP.

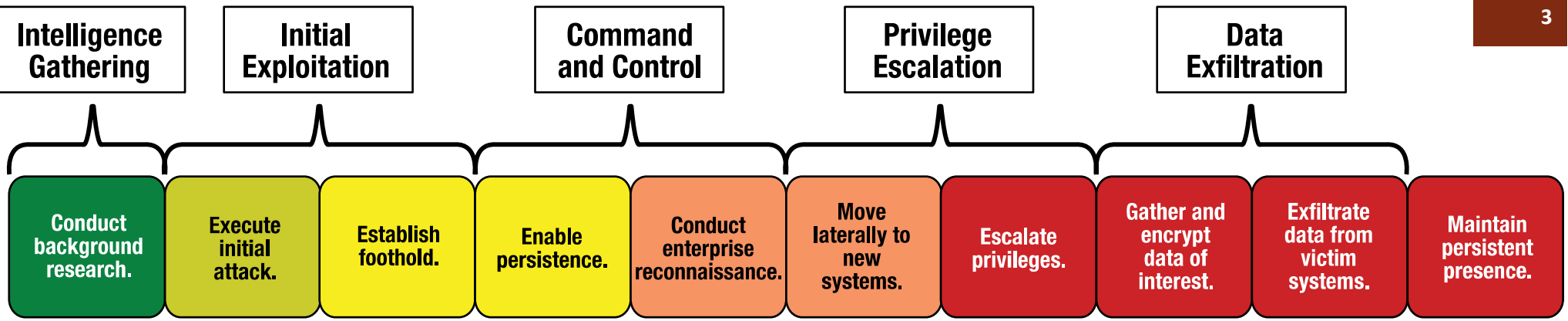


1980s/1990s ➢ **2012**

- ➢ BrainBoot/Morris Worm
- ➢ Polymorphic Viruses
- ➢ Michelangelo
- ➢ Concept Macro Virus
- ➢ Melissa
- ➢ "I Love You"
- ➢ Anna Kournikova
- ➢ Sircam
- ➢ Code Red and Nimda
- ➢ SQL Slammer
- ➢ Blaster
- ➢ Sobig
- ➢ MyDoom
- ➢ Netsky
- ➢ Sasser
- ➢ Storm botnet
- ➢ Koobface
- ➢ Conflicker
- ➢ Aurora
- ➢ Mariposa
- ➢ Stuxnet
- ➢ WikiLeaks
- ➢ Anonymous
- ➢ LulzSec
- ➢ SpyEye/Zeus
- ➢ Duqu
- ➢ Flame

APT (*Advanced Persistent Threat*)

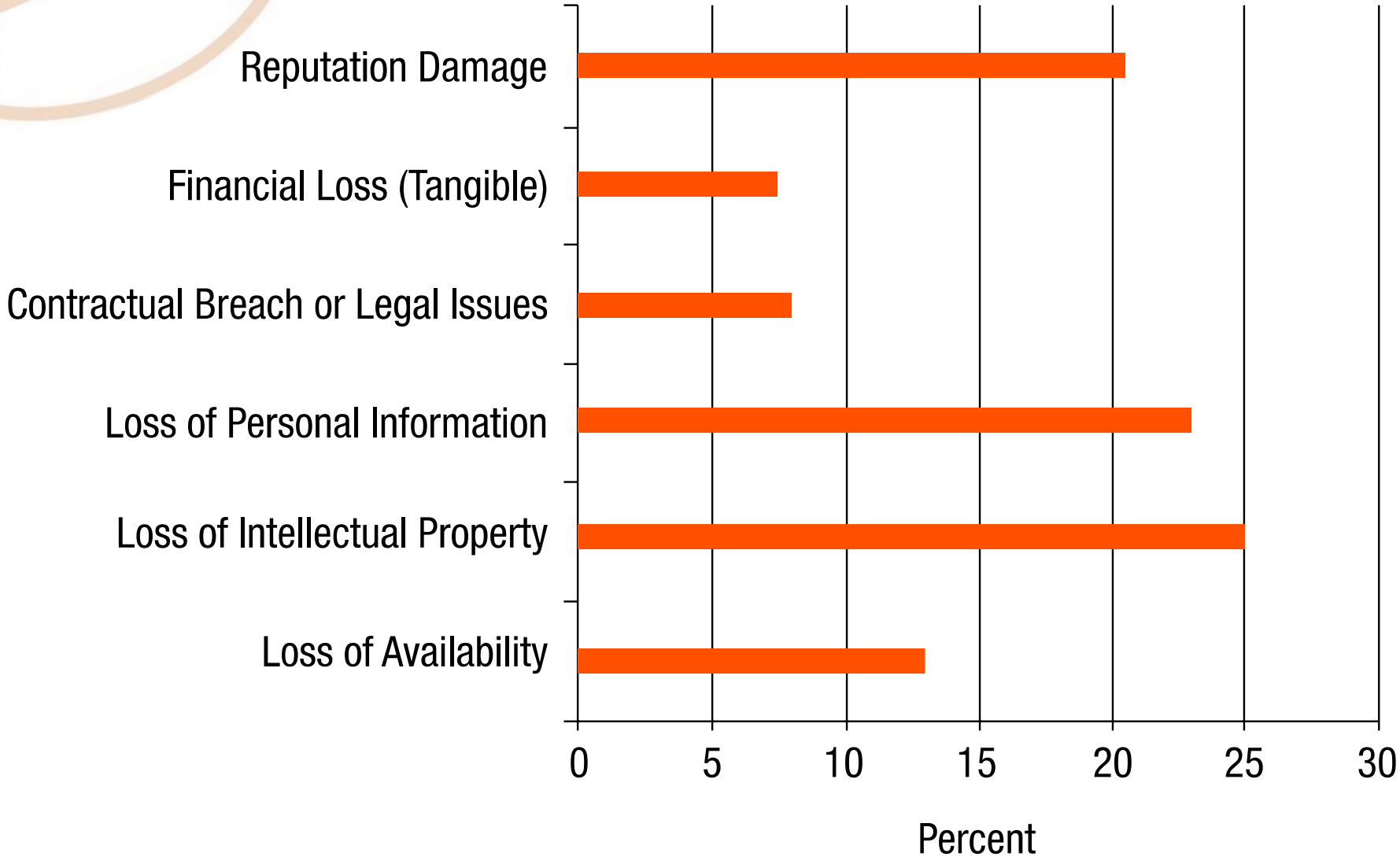
- Un nuevo tipo de atacante
- Atacante que se fija como objetivo una persona u organización a atacar para conseguir un propósito específico



Vectores de ataques adaptativos

- La perspectiva debe ser:
  - La red está comprometida o pronto lo será.
  - ¿Cómo protegeremos los datos más importantes en un entorno comprometido?
  - ¿Cómo hacemos difícil a los atacantes que tengan éxito?
  - ¿Cómo detectamos que se está produciendo un ataque?
  - ¿Cómo responderemos a los ataques sofisticados actuales?

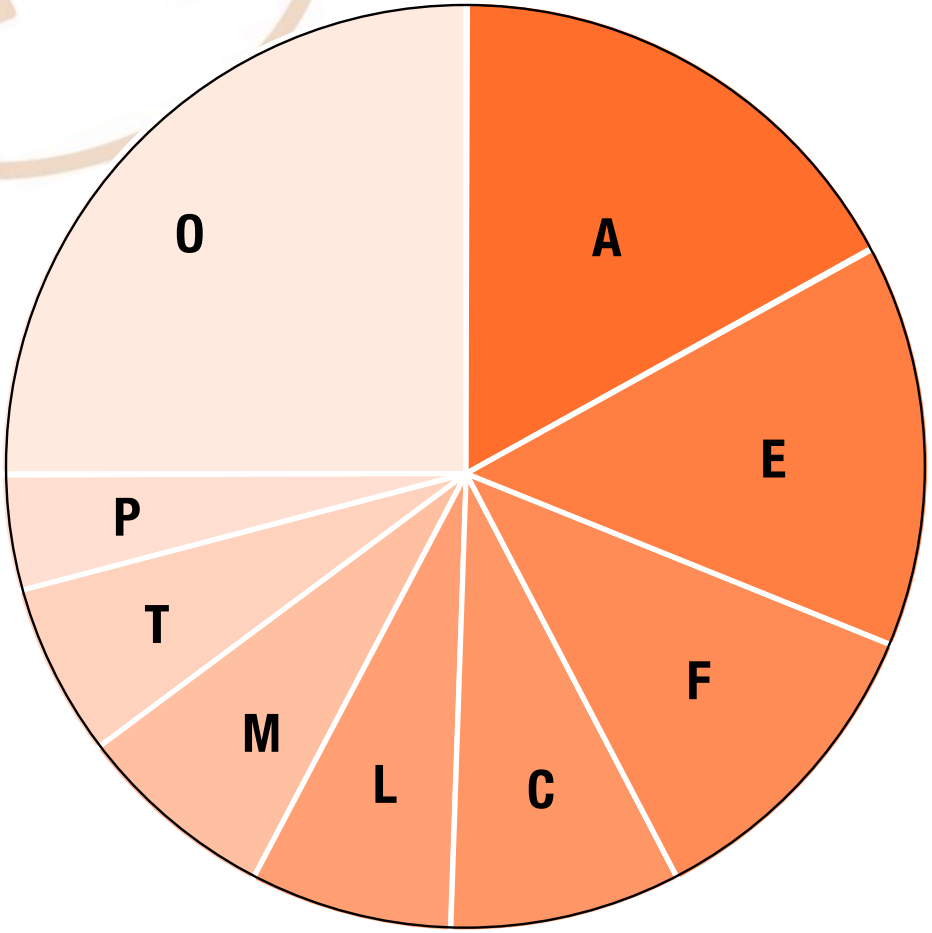
Mayores riesgos de una APT



Fuentes de las APTs

Threat	What They Seek	Business Impact
Intelligence agencies	Political, defense or commercial trade secrets	Loss of trade secrets or commercial, competitive advantage
Criminal groups	Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale	Financial loss, large-scale customer data breach or loss of trade secrets
Terrorist groups	Production of widespread terror through death, destruction and disruption	Loss of production and services, stock market irregularities, and potential risk to human life
Activist groups	Confidential information or disruption of services	Major data breach or loss of service
Armed forces	Intelligence or positioning to support future attacks on critical national infrastructure	Serious damage to facilities in the event of a military conflict

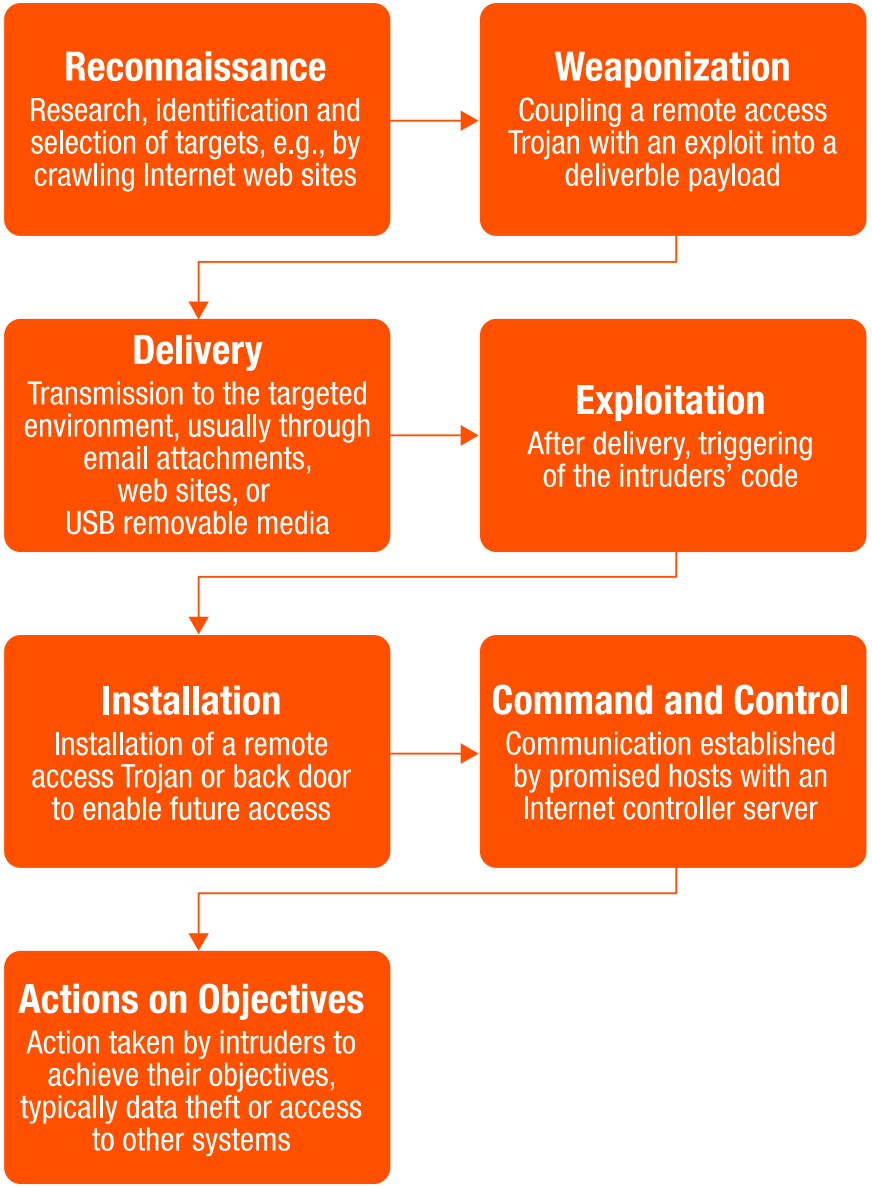
Objetivos de las APTs



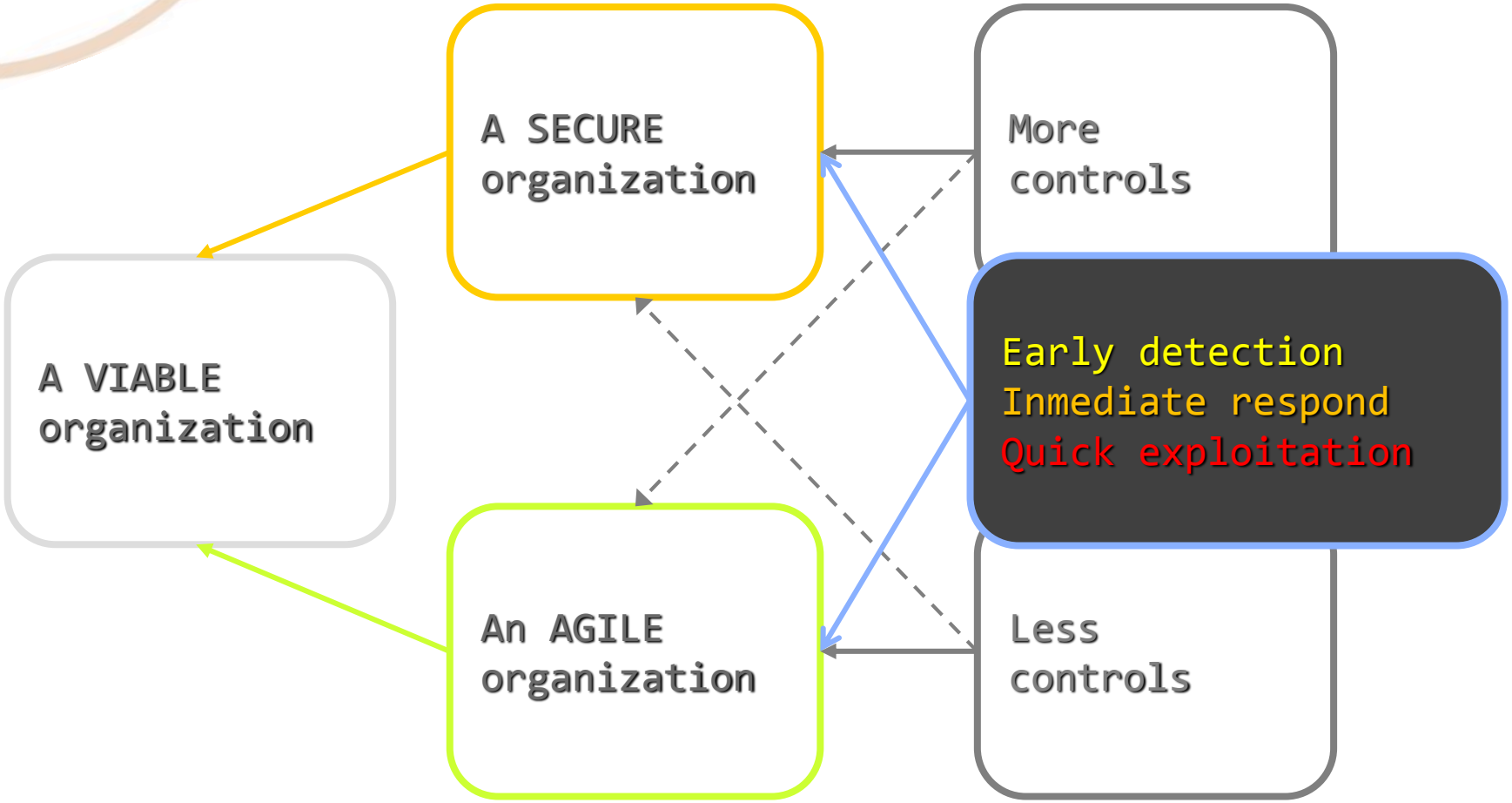
- **A** Aerospace and Defense
- **E** Energy, Oil and Gas
- **F** Finance
- **C** Computer Hardware and Software
- **L** Legal and Consulting Services
- **M** Media and Entertainment
- **T** Telecommunications
- **P** Pharmaceuticals
- **O** Other

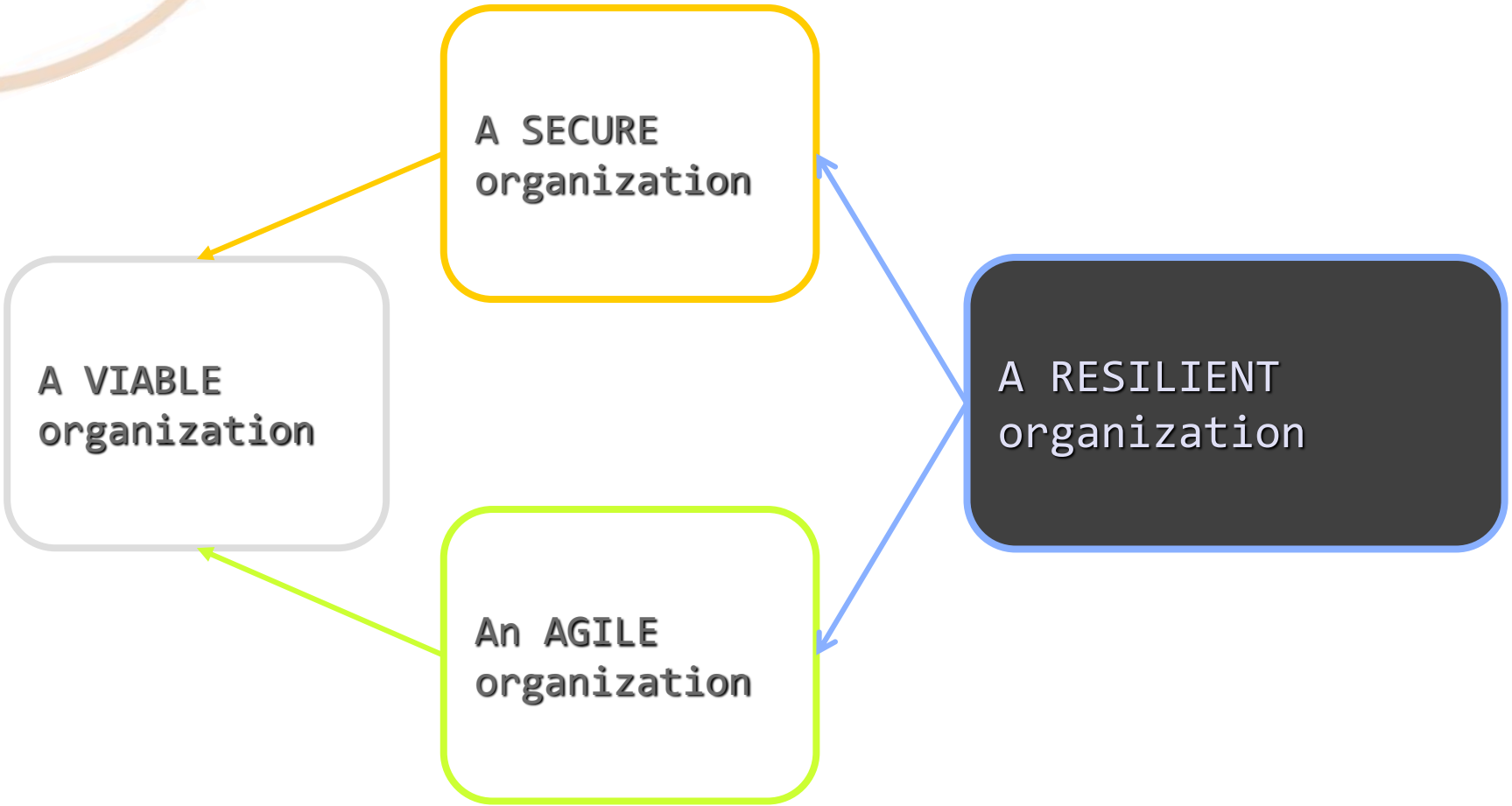
[20] Mandiant, "M-Trends® 2013: Attack the Security Gap™," USA, 2013, *www.mandiant.com/resources/m-trends*

Interrumpir la “kill chain” (Lockheed Martin)

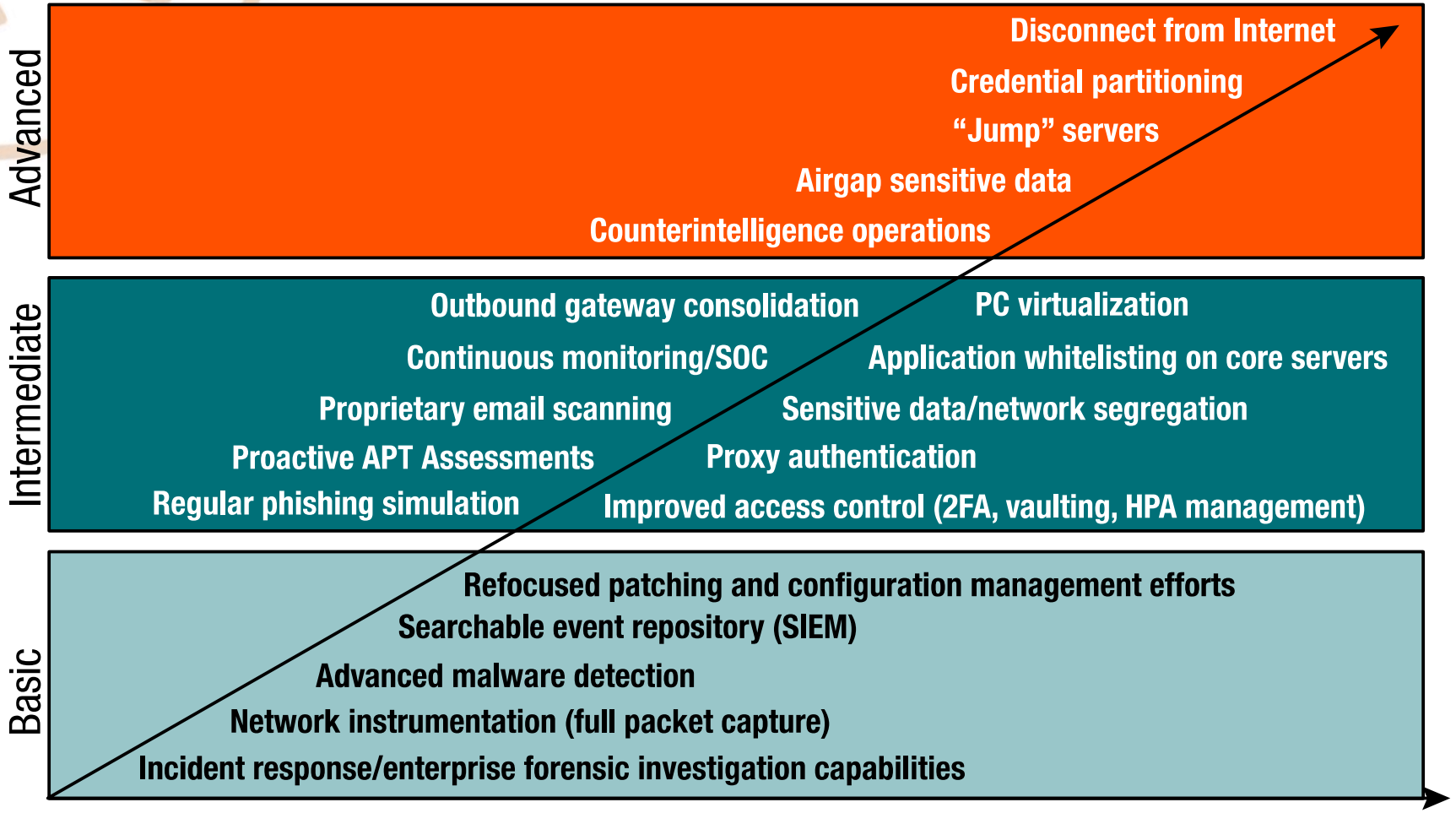



‘Resilience’


A SECURE organization
More controls
A VIABLE organization
Early detection
Inmediate respond
Quick exploitation
An AGILE organization
Less controls

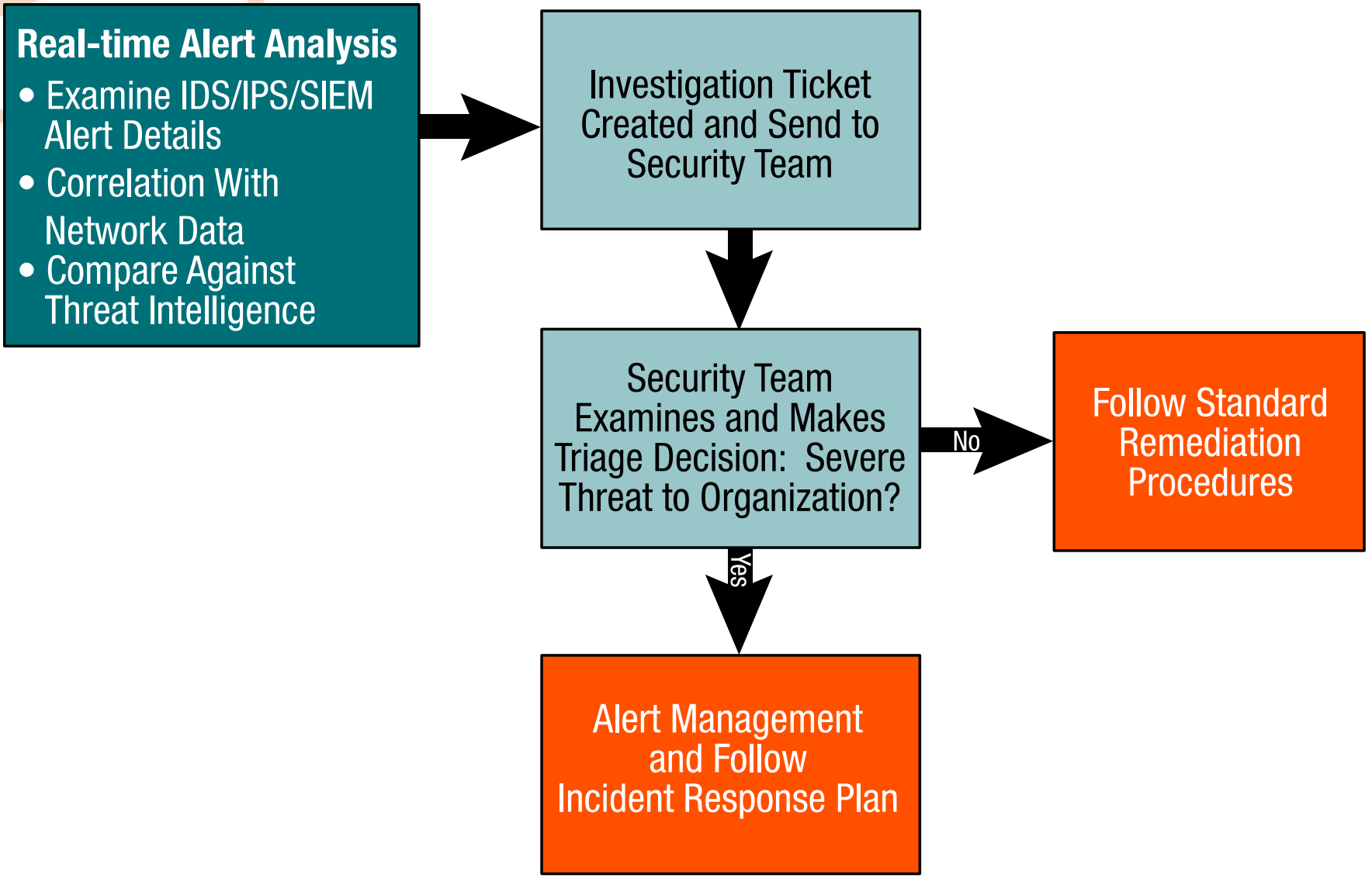

A SECURE organization
A VIABLE organization
A RESILIENT organization
An AGILE organization

Respuesta

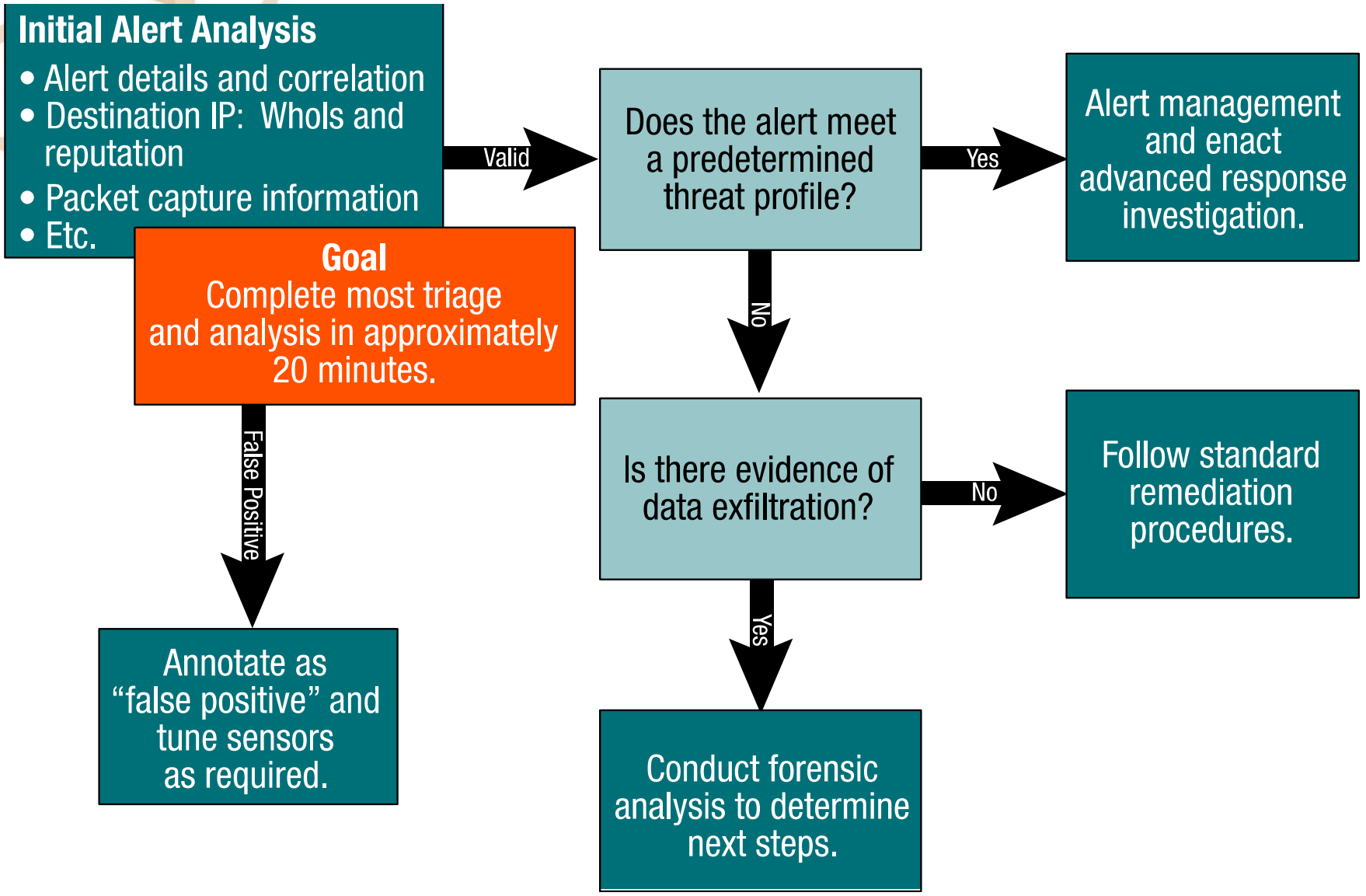


SOC = Security operations center
2FA = Two-factor authentication
HPA = High profile asset
SIEM = Security information and event management

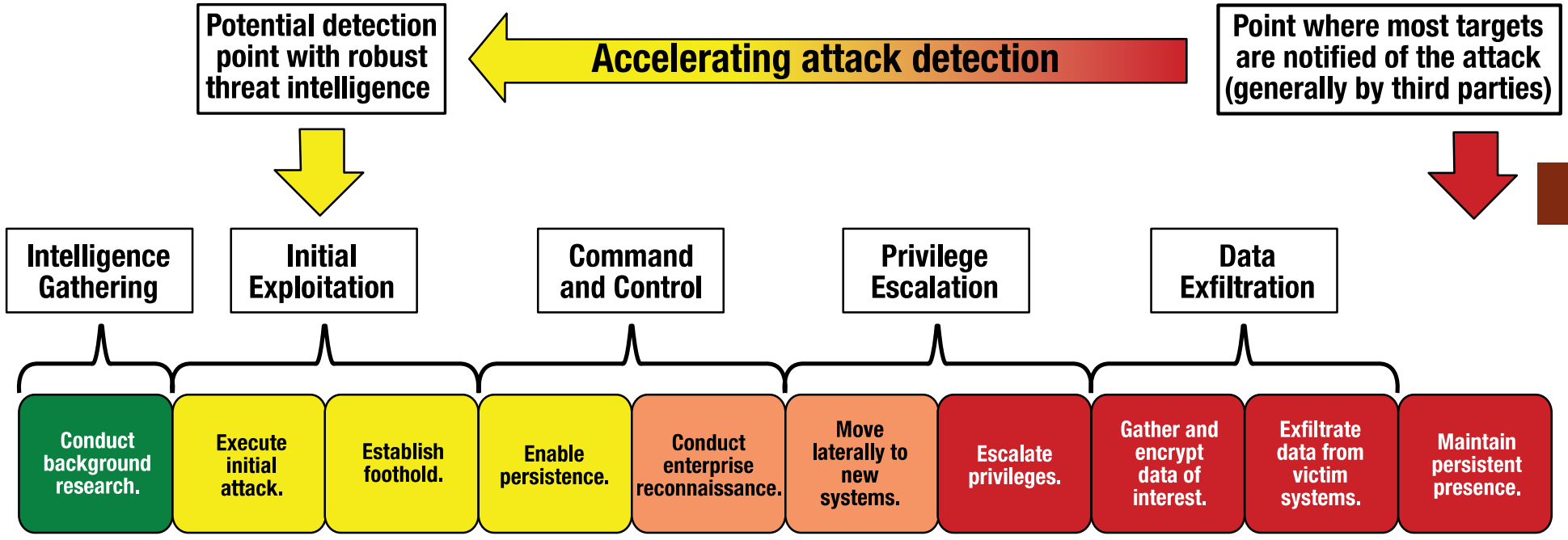
Estandarizar la gestión de incidentes



Estandarizar la gestión de incidentes



Impacto potencial de la ciberinteligencia



El rol del consejo

- 6 preguntas que debería hacer:
  1. ¿Utiliza nuestra organización algún marco de seguridad?
  2. ¿Cuáles son los cinco principales riesgos de la organización en materia de ciberseguridad?
  3. ¿Cómo se conciencia a los empleados sobre su rol en relación a la ciberseguridad?
  4. ¿Se han considerado tanto las amenazas internas como las externas a la hora de planificar las actividades del programa de seguridad?
  5. ¿Cómo es gobernada la seguridad en la organización?
  6. En caso de un incidente serio, ¿se ha desarrollado un protocolo de respuesta robusto?

Referencias

- “Cybersecurity. What The Board Of Directors Needs To Ask”, IIARF Research Report, 2014.
- “Advanced Persistent Threats. How to Manage the Risk to Your Business”, ISACA, 2013.
- “Responding to Targeted Cyberattacks”, ISACA, 2013

… todas ellas accesibles en www.isaca.org/cyber

Thank you…
Keep the conversation at…

@enplusone

@antonio_ramosga

linkedin.com/company/n-1-intelligence-&-research

es.linkedin.com/in/sorani/

http://flip.it/YE7cC

https://plus.google.com/+AntonioRamos